Generalized Inverses of Matrices over Fields of Characteristic Two

John D. Fulton

Department of Mathematical Sciences
Clemson University
Clemson, South Carolina 29631

Dedicated to Alston S. Householder
on the occasion of his seventy-fifth birthday.

Submitted by Emeric Deutsch

ABSTRACT

For F a field of characteristic two, the problem of determining which $m\times n$ matrices of rank r have normalized generalized inverses and which have pseudoinverses is solved. For F_q a finite field of characteristic two, both the number of $m\times n$ matrices of rank r over F which have normalized generalized inverses and the number of $m\times n$ matrices of rank r over F_q which have pseudoinverses are determined.

---

1. INTRODUCTION

Rohde [15, 16] distinguished four different generalized (Moore-Penrose) inverses [11, 12, 14] of a matrix over the complex field—a generalized inverse, a reflexive generalized inverse, a normalized generalized inverse, and the pseudoinverse. Pearl [13] considered the existence of the various generalized inverses of a given $m\times n$ matrix of rank r over an arbitrary field F under an involutory automorphism $\alpha: F\to F$. For F a finite field, the author, in a previous paper [8], enumerated the various generalized inverses of a given $m\times n$, rank r matrix over F. In the same paper, except for fields of characteristic two with α the identity automorphism, the author characterized and enumerated (for F finite) those $m\times n$ matrices of rank r over F with a normalized generalized inverse and with a pseudoinverse. In this paper, the author considers the characterization and the enumeration (F finite) of those $m\times n$ matrices of rank r over F of characteristic two which have a normalized generalized inverse and which have a pseudoinverse, where α is the identity automorphism of F.

 0024-3795/79/060069+8$01.75

2. NOTATION AND PRELIMINARIES

Throughout this paper, F will denote a field of characteristic two, and if designated finite, F_q will denote the Galois field GF (q), $q=2^w$. $M_{m,n}(F)$ will denote the set of all $m\times n$ matrices over F. If $A=(a_{ij})\in M_{m,n}(F)$, then $A^t=(a^t_{ij})\in M_{m,n}(F)$ denotes the transpose of A.

Definition 2.1. Let $A\in M_{m,n}(F)$. Any X in $G(m,n,F)=\{X\in M_{n,m}(F):AXA=A\}$ will be called a *generalized inverse* of A. Any X in $R(m,n,F)=\{X\in G(m,n,F):XAX=X\}$ will be called a *reflexive generalized inverse* of A. Any X in $N(m,n,F)=\{X\in R(m,n,F):(AX)^t=AX\}$ will be called a *normalized generalized inverse* of A and will be denoted by $A^n=X$. Any X in $P(m,n,X)=\{X\in N(m,n,F)$: $(XA)^t=XA\}$ will be called a *pseudo-inverse* of A and will be denoted by $A^+=X$.

Penrose [14] showed that every matrix A over the complex field has an A^n and a unique A^+. However, Pearl [13] showed that the $m\times n$ matrix A of rank r over an arbitrary field has an A^n and an A^+ (unique) only under certain conditions. For later reference, Pearl's result is restated as Theorem 1.

Theorem 1. *Suppose A is an $m\times n$ matrix of rank r over F. Then*

$$A \text{ has an } A^n \quad \text{if and only if} \quad r=\operatorname{rank}(A^tA), \tag{2.1}$$

and

$$A \text{ has an } A^+ \quad \text{if and only if} \quad r=\operatorname{rank}(A^tA)=\operatorname{rank}(AA^t). \tag{2.2}$$

Thus, for example, the $1\times n$ matrix $A=[1,0,\dots,0]$ of rank 1 over GF (2) has both an A^n and an A^+, while the matrix $B=[1,1,0,\dots,0]$ has a B^n but not a B^+, and the matrix B^t has neither.

In order to enumerate, for F finite, those matrices A of rank r in $M_{m,n}(F)$ such that A^n exists and A^+ exists, certain cardinalities are required. In particular, for

$$G_k=\begin{bmatrix} 0 & I_k \\ I_k & 0 \end{bmatrix},$$

where I_k is the $k \times k$ identity matrix, and for $u=2k$, the cardinality $|\mathrm{Sp}_u(q)|$ of the *symplectic group*,

$$\mathrm{Sp}_u(q)=\{P\in M_{u,u}(F) : PG_kP^t=G_k\},$$

is required. Dickson [6] gave $|\mathrm{Sp}_u(q)|$ as

$$|Sp_u(q)|=(q^k-1)q^{k-1}(q^{k-2}-1)q^{k-3}\cdots(q^2-1)q. \tag{2.3}$$

MacWilliams [10] gave the cardinality $|\mathcal{G}_k(q)|$ of the group

$$\mathcal{G}_k(q)=\{P\in M_{k,k}(F) : P^tP=I_k\}$$

$$|\mathcal{G}_k(q)|=\begin{cases} q^v\prod_{i=0}^{v-1}(q^{2v}-q^{2i}) & \text{if} \quad k=2v+1, \\ q^v\prod_{i=1}^{v-1}(q^{2v}-q^{2i}) & \text{if} \quad k=2v. \end{cases} \tag{2.4}$$

Landsberg [9] determined the number $g(n,m,r,q)$ of $n\times m$ matrices of rank r over finite field F_q to be

$$g(n,m,r,q)=q^{r(r-1)/2}\prod_{i=1}^{r}\frac{(q^{n-i+1}-1)(q^{m-i+1}-1)}{(q^i-1)}. \tag{2.5}$$

In a series of papers, Buckhiester [2, 3, 4, 5], by applying the theory of symmetric bilinear forms, found the number $\mathfrak{M}(A,C,n,s,r)$ of $n\times s$ matrices X of rank r over a finite field F_q such that

$$X^tAX=C, \tag{2.6}$$

where A is $n\times n$, symmetric of rank m over F_q, and where C is $s\times s$, symmetric of rank u over F_q. The particular values required are $\mathfrak{M}(I_k,I_r,k,r,r)$ and $\mathfrak{M}(I_k,G_v,k,r,r)$, where for $r=2v$,

$$G_v=\begin{bmatrix} 0 & I_v \\ I_v & 0 \end{bmatrix}.$$

Buckhiester [4] determined $\mathfrak{M}(I_k,I_r,k,r,r)$ to be

$$\mathfrak{M}(I_k,I_r,k,r,r)=q^{k-r}\mathcal{P}(r-1,k), \tag{2.7}$$

where

$$\mathcal{P}(r,k)=\begin{cases}\prod_{i=1}^{r/2}(q^{k-2i}-1)(q^{k-2i+1}) & (k \text{ even}, r \text{ even}),\\ q^{k-r}\prod_{i=1}^{(r-1)/2}(q^{k-2i}-1)(q^{k-2i+1}) & (k \text{ even}, r \text{ odd}),\\ \prod_{i=1}^{r/2}(q^{k-2i})(q^{k-2i+1}-1) & (k \text{ odd}, r \text{ even}),\\ (q^{k-r}-1)\prod_{i=1}^{(r-1)/2}(q^{k-2i+1}-1)(q^{k-2i}) & (k \text{ odd}, r \text{ odd}).\end{cases} \tag{2.8}$$

Buckhiester [3] also determined $\mathfrak{M}(I_k,G_v,k,r,r)$, for $r=2v$, to be

$$\mathfrak{M}(I_k,G_v,k,r,r)=\mathfrak{M}(I_k,0,k,r,r)\prod_{i=1}^{v}q^{k-v-i}, \tag{2.9}$$

where $\mathfrak{M}(I_k,0,k,r,r)$ is given by

$$\mathfrak{M}(I_k,0,k,r,r)=\begin{cases}\prod_{i=1}^{v}(q^{k-i}-q^{i-1}) & (k \text{ odd}),\\ \prod_{i=1}^{v}(q^{k-i}-q^{i}) & (k \text{ even}).\end{cases} \tag{2.10}$$

3. MATRICES OVER F WHICH POSSESS NORMALIZED GENERALIZED INVERSES

The remarks which follow will be summarized as Theorem 2.

Frame [7] has shown (and it is an easy exercise to verify) that the $m\times n$ matrix A has rank r if and only if A can be factored as

$$A=RS, \tag{3.1}$$

where R is $m\times r$ of rank r and were S is $r\times n$ of rank r. Moreover, for A $m\times n$ of rank r over F factored as in (3.1), $\operatorname{rank}(A^tA)=r$ if and only if $\operatorname{rank}(R^tR)=r$. Thus by (2.1), the $m\times n$ matrix A of rank r has a normalized generalized inverse if and only if A can be factored as (3.1), where $r=\operatorname{rank}R$ $=\operatorname{rank}R^tR$ and where $r=\operatorname{rank}S$.

Two cases are distinguished. Either $B=R^tR$ is *alternate* or else it is *nonalternate*. If $B=R^tR$ is $r\times r$ of rank r and *alternate*, then r is even $(r=2k)$, and there exists P nonsingular such that

$$X^tX=(RP)^t(RP)=P^tBP=\begin{bmatrix} 0 & I_k \\ I_k & 0 \end{bmatrix}=G_k, \tag{3.2}$$

where $X=RP$. Conversely, if the $m\times r$ matrix X over F satisfies $X^tX=G_k$, then for each nonsingular P of size r, $R=XP$ satisfies $R^tR=(XP)^t(XP)=P^tG_kP=B$, where $B=R^tR$ is alternate [1] of rank r.

Thus, if R is $m\times r$ of rank r over F such that R^tR is alternate of rank r, then $R=XP$, where X is $m\times r$ such that $X^tX=G_k$ and where P is $r\times r$ and nonsingular. Hence, for such an R and any $r\times n$ matrix S of rank r, $A=RS$ has a normalized generalized inverse. But $RS=(XP)S=X(PS)=XS_1$, where $S_1=PS$ is $r\times n$ or rank r.

Finally, if each of X_1 and X_2 is $m\times r$ over F such that $X_1^tX_1=X_2^tX_2=G_k$, then $X_1S_1=X_2S_2$, for each of S_1 and S_2 $r\times n$ of rank r over F, if and only if $X_1=X_2(S_2S_1^i)=X_2Q$, where S_1 is any right inverse of S_1 and where $Q=S_2S_1$ satisfies $G_k=X_1^tX_1=Q^tX_2^tX_2Q=Q^tG_kQ$, that is, where Q is in the symplectic group $\mathrm{Sp}_r(F)$ over F.

On the other hand, if an $m\times n$ matrix A of rank r over F is factored as $A=RS$, where S is $r\times n$ of rank r and where R is $m\times r$ such that $R^tR=B$ is nonalternate of rank r, then there exists P, $r\times r$ and nonsingular, such that

$$X^tX=(RP)^t(RP)=P^tBP=I_r, \tag{3.3}$$

where $X=RP$. Conversely, if the $m\times r$ matrix over F satisfies $X^tX=I_k$, then for each nonsingular P of size r, $R=XP$ satisfies $R^tR=P^tP=B$, where $B=R^tR$ is nonalternate [1] of rank r.

Therefore, the $m\times n$ matrix $A=RS$ over F has a normalized generalized inverse, where S is $r\times n$ of rank r and where $R=XP$ is $m\times r$ such that $X^tX=I_r$ and P is $r\times r$ nonsingular. Moreover, $S_1=PS$ is $r\times n$ of rank r, and A has the factorization $A=XS$.

Suppose the $m\times n$ matrix A of rank r with normalized generalized inverse has two factorizations as above: $A=X_1S_1=X_2S_2$. Then $X_1=X_2(S_2S_1^i)$ $=X_2B$, where $B=S_2S_1^i$ with S_1^i any right inverse of S_1. Thus, $X_1^tX_1=$

$B^t(X_2^tX_2)B$. If $X_1^tX_1=I_r$, then $X_2^tX_2$ cannot be G_k(for $r=2k$) [1]. Thus, $X_2^tX_2=I_r$ and B is in $\mathcal{G}_r(F)$. If $X_1^tX_1=G_k$ $(r=2k)$, then $X_2^tX_2=G_k$, and B is in $\mathrm{Sp}_r(F)$. Theorem 2 below summarizes these results.

THEOREM 2. *The $m\times n$ matrix A of rank r over F has a normalized generalized inverse if and only if $A=XS$, where S is $r\times n$ of rank r and where X is $m\times r$ such that $X^tX=I_r$ or $X^tX=G_k$ $(r=2k)$. Moreover, the $m\times n$ matrix A of rank r over F with normalized generalized inverse has the factorizations as above, $A=X_1S_1=X_2S_2$, if and only if $X_1=X_2(S_2S_1^i)$, where S_2S_1 is in $\mathcal{G}_r(F)$ if $X_1^tX_1=I_r$ and where $S_2S_1^i$ is in $\mathrm{Sp}_r(F)$ if $X_1^tX_1=G_k(r=2k)$. S_1^i is any right inverse of S_1.*

Let F_q denote the finite field $\mathrm{GF}(q)$. Let $\mathfrak{N}(m,n,r,q)$ be the number of $m\times n$ matrices A of rank r over F_q each of which has a normalized generalized inverse. Then Theorem 2 has the following corollary.

COROLLARY 1. *The number $\mathfrak{N}(m,n,r,q)$ of $m\times n$ matrices of rank r over F_q each of which has a normalized generalized inverse is*

$$\mathfrak{N}(m,n,r,q)=\begin{cases}\mathfrak{M}(I_m,I_r,m,r,r)\dfrac{g(r,n,r,q)}{|\mathcal{G}_r(q)|}, & r=2k+1\\[2ex] \left[\dfrac{\mathfrak{M}(I_m,I_r,m,r,r)}{|\mathcal{G}_r(q)|}+\dfrac{\mathfrak{M}(I_m,G_k,m,r,r)}{|\mathrm{Sp}_r(q)|}\right]g(r,n,r,q), & r=2k,\end{cases}$$

where $\mathfrak{M}(I_m,I_r,m,r,r)$ is given by (2.7), *$\mathfrak{M}(I_m,G_k,m,r,r)$ by* (2.9), *$|\mathcal{G}_r(q)|$ by* (2.4), *$|\mathrm{Sp}_r(q)|$ by* (2.3) *and $g(r,n,r,q)$ by* (2.5).

4. MATRICES OVER F WHICH POSSESS PSEUDOINVERSES

The remarks below are summarized as Theorem 3, which follows.

By (2.2) of Theorem 1, the $m\times n$ matrix A of rank r over F has a pseudoinverse if and only if A has a normalized generalized inverse and $r=\mathrm{rank}(AA^t)$. Thus, let the $m\times n$ matrix A of rank r over F be factored as $A=XS$, where X is $m\times r$ such that X^tX is either G_k ($r=2k$ in this case) or I_r, and S is $r\times n$ of rank r. Now $r=\mathrm{rank}(AA^t)$ if and only if $r=\mathrm{rank}(SS^t)$. Let $C=SS^t$. Then C is $r\times r$ and symmetric.

If $r=2k$ and C is alternate, there exists P nonsingular such that $YY^t=(PS)(PS)^t=PCP^t=G_k$. That is, there exists P nonsingular such that $Y=PS$ satisfies $YY^t=G_k$. Conversely, suppose $S=P^{-1}Y$ is $r\times n$ such that $YY^t=G_k$, and suppose X is $m\times r$ such that X^tX is I_r or G_k. Then $SS^t=P^{-1}G_k(P^{-1})^t$. Thus, SS^t is alternate [1] of rank r. Moreover, the $m\times n$ matrix $A=XP^{-1}Y$ has rank r and has a pseudoinverse.

Similarly, it can be shown that the $m\times n$ matrix $A=XS$ of rank r over F with normalized generalized inverse, where SS^t is alternate, has a pseudoinverse if and only if $S=QY$, where Q is $r\times r$ nonsingular and where $YY^t=I_r$.

Thus, the $m\times n$ matrix A of rank r over F has a pseudoinverse if and only if A can be factored as $A=XQY$, where X is $m\times r$ such that X^tS is I_r or G_k $(r=2k)$, Q is $r\times r$ nonsingular, and Y is $r\times n$ such that YY^t is I_r or G_k $(r=2k)$. Moreover, since by Theorem 1 such an $m\times n$ matrix A of rank r over F has a normalized generalized inverse, A has the factorizations as above, $A=X_1Q_1Y_1=X_2Q_2Y_2$, if and only if $X_1=X_2B$, where $B=Q_2Y_2Y_1^tQ_1^{-1}$ is in $\mathcal{G}_r(F)$ if $X_1^tX_1=I_r$ and where B is in $\mathrm{Sp}_r(F)$ $(r=2k)$ if $X_1^tX_1=G_k$. However, if A with pseudoinverse has the factorizations as above, $A=X_1Q_1Y_1=X_2Q_2Y_2$, where there exists no B in $\mathcal{G}_r(F)$ or in $\mathrm{Sp}_k(F)$ such that $X_1=X_2B$, then $X_1=X_2$ and $Q_1Y_1=Q_2Y_2$. But $Q_1Y_1=Q_2Y_2$ if and only if $Y_1=(Q_1^iQ_2)Y_2$, where Q_1^i is any left inverse of Q_1, where $Q_1^iQ_2$ is in $\mathcal{G}_r(F)$ if $Y_1Y_1^t=I_r$, and where $Q_1^iQ_2$ is in $\mathrm{Sp}_r(F)$ if $Y_1Y_r^t=G_k$.

Theorem 3 summarizes these results.

THEOREM 3. *The $m\times n$ matrix A of rank r over F has a pseudoinverse if and only if A can be factored as $A=XQY$, where X is $m\times r$ such that X^tX is I_r or G_k ($r=2k$ in this case), where Q is $r\times r$, nonsingular, and where YY^t is I_r or G_k. Moreover, if the $m\times r$ matrices X such that $X^tX=I_r$ or $X^tX=G_k$ have been chosen so that no $X_1=X_2B$ for B in $\mathcal{G}_r(F)$ or in $\mathrm{Sp}_r(F)$, then the $m\times n$, rank r matrix A with pseudoinverse has the factorizations as above, $A=X_1Q_1Y_1=X_2Q_2Y_2$, if and only if $X_1=X_2$ and $Y_1=CY_2$, where $C=Q_1^iQ_2$ is in $\mathcal{G}_r(F)$ if $Y_1Y_1^t=I_r$ and where C is in $\mathrm{Sp}_r(F)$ if $Y_1Y_1^t=G_k$. Q_1^i is any left inverse of Q_1.*

Let us consider the finite field F and let $\mathcal{P}(m,n,r,q)$ be the number of $m\times n$ matrices of rank r over F_q which have pseudoinverses. Hence, Theorem 3 has the following corollary.

COROLLARY 2. *The number of $m\times n$ matrices of rank r over F_q each of which has a pseudoinverse is*

$$\mathcal{P}(m,n,r,q)=\begin{cases}\dfrac{\mathfrak{M}(I_m,I_r,m,r,r)\,\mathfrak{M}(I_n,I_r,n,r,r)\,g(r,r,r,q)}{|\mathcal{G}_r(q)|^2}, & r \text{ odd}\\[2ex] \left[\dfrac{\mathfrak{M}(I_m,I_r,m,r,r)}{|\mathcal{G}_r(q)|}+\dfrac{\mathfrak{M}(I_m,G_k,m,r,r)}{|\mathrm{Sp}_r(q)|}\right]g(r,r,r,q) & \\ \times\left[\dfrac{\mathfrak{M}(I_n,I_r,n,r,r)}{|\mathcal{G}_r(q)|}+\dfrac{\mathfrak{M}(I_n,G_k,n,r,r)}{|\mathrm{Sp}_r(q)|}\right], & r=2k,\end{cases}$$

where $\mathfrak{M}(I_m, I_r, m, r, r)$ *and* $\mathfrak{M}(I_n, I_r, n, r, r)$ *are given by* (2.7) *and* (2.8), *where* $\mathfrak{M}(I_m, G_k, m, r, r)$ *and* $\mathfrak{M}(I_n, G_k, n, r, r)$ *are given by* (2.9) *and* (2.10), *where* $|\mathcal{G}_r(q)|$ *is given by* (2.4), *where* $|\mathrm{Sp}_r(q)|$ *is given by* (2.3), *and where* $g(r,r,r,q)$ *is given by* (2.5).

The author intends in subsequent papers to consider problems related to generalized inverses of matrices over modular rings of integers and over finite local rings, the building blocks for the finite commutative rings with identity.

REFERENCES

1 A. A. Albert, Symmetric and alternate matrices in an arbitrary field, I, *Trans. Amer. Math. Soc.* 43:386–436 (1938).
2 P. G. Buckhiester, Rank r solutions to the matrix equation $XAX^t = C$, A alternate, over $GF(2^y)$, *Amer. Math. Soc. Trans.* 189:201–209 (1974).
3 P. G. Buckhiester, Rank r solutions to the matrix equation $XAX^t = C$, A nonalternate, C alternate, over $GF(2^y)$, *Canad. J. Math.* 26:78–90 (1974).
4 P. G. Buckhiester, The number of solutions to the matrix equation $XAX^t = C$, A and C nonalternate and of full rank, over $GF(2^y)$, *Math. Nachr.* 63:37–41 (1974).
5 P. G. Buckhiester, Rank r solutions to the matrix equation $XAX^t = C$, A and C nonalternate over $GF(2^y)$, *Math. Nachr.* 63:413–422 (1974).
6 L. Dickson, *Linear Groups*, Leipzig (1901); Dover, 1958.
7 J. S. Frame, Matrix functions and applications, *IEEE Spectrum* 1:208–220 (1964).
8 J. D. Fulton, Generalized inverses of matrices over a finite field, *Discrete Math.* 21:23–29 (1978).
9 G. Landsberg, Ueber eine Anzahlbestimmung und eine damit zusammenhangende Reihe, *J. Reine Angew. Math.* 111:87–88 (1893).
10 J. MacWilliams, Orthogonal matrices over finite fields, *Amer. Math. Monthly* 76:152–164 (1969).
11 E. H. Moore, On the reciprocal of the general algebraic matrix (abstract), *Bull. Amer. Math. Soc.* 26:394–395 (1920).
12 E. H. Moore, General analysis, part I, *Mem. Amer. Philos. Soc.* I (1935).
13 M. H. Pearl, Generalized inverses of matrices with entries taken from an arbitrary field, *Linear Algebra and Appl.* 1:571–587 (1968).
14 R. Penrose, A generalized inverse of matrices, *Proc. Cambridge Philos. Soc.* 51:406–413 (1955).
15 C. A. Rohde, Generalized inverses of partitioned matrices, *J. Soc. Indust. Appl. Math.* 13:1033–1035 (1965).
16 C. A. Rohde, Some results on generalized inverses, *SIAM Rev.* 8:201–205 (1966).

Received 23 May 1978; revised 1 December 1978